CLAIMS

1. In a computing system, a method of operation comprising:

   receiving a first permutation specification of a first permutation of a first plurality of inputs;

   receiving a first permutation modifier;

   receiving an interaction specification of a first interaction between the first permutation and the first permutation modifier; and

   generating a second permutation specification of a second permutation of the first plurality of inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier.

2. The method of claim 1 wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

3. The method of claim 1 wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of inputs.

4. The method of claim 3 wherein the third permutation specification specifies the third permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values

specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

5. The method of claim 3 wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the inputs to the third permutation.

6. The method of claim 3 wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

7. The method of claim 1 wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

8. The method of claim 1 wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

9. The method of claim 1 wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first permutation are moved to be outputs immediately to the left of those specified in the first interaction specification..

10. The method of claim 1 wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

11. The method of claim 1 wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

12. The method of claim 1 wherein the first and second permutations comprise 32 bit permutations.

13. The method of claim 1 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification.

14. The method of claim 13 further comprising configuring the programmable cryptography engine based at least in part on the generated configuration vector.

15. The method of claim 1 further comprising:

receiving a second permutation modifier;

receiving a second interaction specification of a second interaction between the second permutation and the second permutation modifier;

generating a third permutation specification of a third permutation of the first plurality of inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier.

16. The method of claim 15 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the third permutation specification.

17. A computer readable medium comprising:

a storage medium; and

a plurality of executable instructions designed to program a computing device to enable the computing device to:

receive a first permutation specification of a first permutation of a first plurality of inputs;

receive a first permutation modifier;

receive an interaction specification of a first interaction between the first permutation and the first permutation modifier; and

generate a second permutation specification of a second permutation of the first plurality of inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier.

18. The computer readable medium of claim 17 wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

19. The computer readable medium of claim 17 wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of inputs.

20. The computer readable medium of claim 19 wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the inputs to the third permutation.

21. The computer readable medium of claim 19 wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

22. The computer readable medium of claim 17 wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

23. The computer readable medium of claim 17 wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

24. The computer readable medium of claim 17 wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first

permutation are moved to be outputs immediately to the left of those specified in the first interaction specification..

25. The computer readable medium of claim 17 wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

26. The computer readable medium of claim 17 wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

27. The computer readable medium of claim 17 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification.

28. The computer readable medium of claim 27 further comprising configuring the programmable cryptography engine based at least in part on the generated configuration vector.

29. The computer readable medium of claim 17 further comprising:

receiving a second permutation modifier;

receiving a second interaction specification of a second interaction between the second permutation and the second permutation modifier;

generating a third permutation specification of a third permutation of the first plurality of inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier.

30. The computer readable medium of claim 29 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the third permutation specification.

31. A computing device comprising:

storage medium having stored therein a first plurality of executable instructions designed to:

receive a first permutation specification of a first permutation of a first plurality of inputs;

receive a first permutation modifier;

receive an interaction specification of a first interaction between the first permutation and the first permutation modifier; and

generate a second permutation specification of a second permutation of the first plurality of inputs, the second permutation resulting from the first permutation and the first permutation modifier reflective of the specified first interaction between the first permutation and the first permutation modifier; and

at least one processor coupled to the storage medium to execute the instructions.

32. The computing device of claim 17 wherein the first permutation specification specifies the first permutation by specifying values comprising a plurality of input sources for a plurality of outputs in an ordered manner, where positions of the specified values specify the outputs, and the specified values correspondingly identify the input sources of the outputs.

33. The computing device of claim 17 wherein the first permutation modifier comprises a third permutation specification of a third permutation of a second plurality of inputs.

34. The computing device of claim 19 wherein the first interaction specification comprises an 'into' interaction between the first and third permutation specifications where the outputs of the first permutation are provided as the inputs to the third permutation.

35. The computing device of claim 19 wherein the first interaction specification comprises a 'concatenate' interaction adjacently joining the first and third permutations.

36. The computing device of claim 17 wherein the first interaction specification comprises a 'rotate right' interaction where outputs of the first permutation are moved to be outputs immediately to the right of those specified in the first interaction specification.

37. The computing device of claim 17 wherein the first interaction specification comprises a 'select' interaction where the second permutation comprises a subset of the first permutation.

38. The computing device of claim 17 wherein the first interaction specification comprises a 'rotate left' interaction where outputs of the first permutation are moved to be outputs immediately to the left of those specified in the first interaction specification..

39. The computing device of claim 17 wherein the first interaction specification comprises a 'pad' interaction where the second permutation specification is obtained by padding the first permutation specification.

40. The computing device of claim 17 wherein the first permutation modifier is null and the first interaction specification comprises an 'inverse' interaction where the outputs of the second permutation comprise output position numbers of the first permutation for the corresponding output position of the second permutation.

41. The computing device of claim 17 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the second permutation specification.

42. The computing device of claim 41 further comprising configuring the programmable cryptography engine based at least in part on the generated configuration vector.

43. The computing device of claim 17 further comprising:

receiving a second permutation modifier;

receiving a second interaction specification of a second interaction between the second permutation and the second permutation modifier;

generating a third permutation specification of a third permutation of the first plurality of inputs, the third permutation resulting from the second permutation and the second permutation modifier reflective of the specified second interaction between the second permutation and the second permutation modifier.

44. The computing device of claim 43 further comprising generating a configuration vector to configure a programmable cryptography engine based at least in part on the third permutation specification.